



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/679,333	10/04/2000	Stefan Hepper	DE919990073US1	6558

7590 08/10/2004

Kevin P Radigan Esq
Heslin & Rothenberg PC
5 Columbia Circle
Albany, NY 12203

EXAMINER

LANIER BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/10/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/679,333

Applicant(s)

HEPPER ET AL.

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 October 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 3, 7, 11, 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claim 3 recites the limitation "creation from the two random numbers and the transmitted key of a session key". There is no determination of what is being created.
4. Claim 3 recites the limitation "the encrypted random numbers" in lines 13-14. There is insufficient antecedent basis for this limitation in the claim.
5. Claim 7 recites the limitation "chipcard identification data" in lines 14-15. There is insufficient antecedent basis for this limitation in the claim.
6. Claim 11 is indefinite because it does not properly define what an "APDU structure" is.
7. Claim 16 recites the limitation "the random number " in line 15. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

Art Unit: 2132

subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1, 4, 6, 8, 12-15, 17, 18, 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Peyret, U.S. Patent No. 5,923,884. Referring to claims 1, 4, 6, 12-15, 17, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client, and unpacking of the data packet and transmission of the individual commands in sequence to the chipcard. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct.

Referring to claim 8, Peyret discloses that the cryptosystem used can be a public key cryptosystem (asymmetrical) (Col. 5, lines 31-33).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. Claims 2, 7, 10, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Everett, U.S. Patent No. 6,575,372. Referring to claims 2, 7, 10, 19, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates

Art Unit: 2132

the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client, and unpacking of the data packet and transmission of the individual commands in sequence to the chipcard. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct. Peyret does not disclose that the keys are generated based on card identification data. Everett discloses an IC card loading system wherein to generate cryptographic keys for each individual IC card, a certificate authority uses card identification information transmitted from the terminal in order to generate individual key sets for the IC cards (Col. 5, lines 42-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the cryptographic keys of Peyret to be generated based on the IC card identification data in order to easily identify and authenticate the cards at a later point in time as taught in Everett (Col. 8, lines 25-34).

13. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Hanel, GB 2,314,948. Referring to claim 16, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of

Art Unit: 2132

the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client, and unpacking of the data packet and transmission of the individual commands in sequence to the chipcard. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct. Peyret does not disclose using message authentication codes in the command codes. Hanel discloses a chipcard data transfer method wherein message authentication codes are appended to commands (Page 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the commands of Peyret to include a MAC because it is a known procedure as disclosed in Hanel (Page 1).

14. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Klingman, U.S. Patent No. 5,729,594. Referring to claim 5, Peyret discloses a method for loading applications onto a smart card wherein the system includes a smart card, terminal (client), and a server (Fig. 4). The smart card has a first interface system that

Art Unit: 2132

may connect the smart card to the terminal and second interface to connect the terminal to the server (Fig. 4 & Col. 7, lines 33-39). When the smart card is connected to the terminal, the processor of the smart card, verifies the authenticity of the terminal and of the server and visa versa. If the server and the smart card authenticate each other, then the loader within the smart card begins the loading process (Col. 7, lines 42-67). Once an application is selected, which meets the limitation of loading a sequence of commands to download the application component to the chipcard, to be loaded the smart card authenticates the application code through the use of digital signatures (Col. 9, lines 50-53). Digital signatures utilize private or secret keys, which meet the limitation of delivery of a secret key or session key by the server, generation of a digital signature with the secret key or session key by way of each command within the command sequence, transmission of the signed command sequence as a data packet to the client, and unpacking of the data packet and transmission of the individual commands in sequence to the chipcard. If the digital signature is valid then the application is loaded onto the smart card (Col. 9, lines 54-57), which meets the limitation of checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct. Peyret does not disclose communication using SSL. Klingman discloses client server communications using SSL (Col. 3, lines 32-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use SSL in the communications of Peyret in order to provide a secure communication line as taught in Klingman (Col. 3, lines 37-39).

15. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peyret, U.S. Patent No. 5,923,884, in view of Schneier. Referring to claim 9, Peyret discloses the use of public key cryptography but does not disclose the use of RSA. Schneier discloses that RSA is a form of

Art Unit: 2132

public key cryptography (Page 366). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use RSA as the public key cryptographic method in Peyret because RSA is the most popular form of public key cryptography as disclosed in Schneier (Page 366-367).

Conclusion


16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100